COUNTY OF LOS ANGELES

CHIEF INFORMATION OFFICE

500 WEST TEMPLE STREET
493 HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

TELEPHONE: (213) 974-2008
FACSIMILE: (213) 633-4733

June 24, 2003

To: Supervisor Yvonne Brathwaite Burke, Chair
Supervisor Don Knabe, Chair Pro Tem
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Michael D. Antonovich

From: Jon W. Fullinwider
Chief Information Officer

Subject: **HIJACKING OF COUNTY OF LOS ANGELES INTERNET ADDRESSES**

On May 1, 2003, the Internal Services Department (ISD) was notified by an individual from the United Kingdom that County Internet addresses were being used for unauthorized purposes including the sending of Spam, pornographic materials, and hacking attacks.

Upon notification, ISD began an internal investigation, took corrective actions to regain control of the affected addresses, and implemented mitigation initiatives to ensure a similar event does not occur in the future.

The ISD networking organization determined that the national Internet registration authority allowed the Internet addresses and the corresponding owner name (County of Los Angeles) to be changed to a bogus company doing business as Atriva. When ISD contacted Atriva, the telephone number provided was the number for a UPS store in Pleasanton, California. The American Registry of Internet Numbers (ARIN) is the coordinating entity for the management and coordination of Internet addresses. ARIN can be accessed by anyone and with, apparently no more than a phone call and a follow-up email, an individual can identify himself as an address owner and request that the Internet address be transferred to another entity. Since ARIN does not have a rigorous method of determining change authority, they allowed ownership of our Internet addresses to be changed by an individual who claimed to be an authorized County representative.

The Auditor-Controller was notified of the incident on May 9, 2003, and is continuing to investigate the details of this event that may lead to legal action being taken if sufficient information can be obtained that would allow for prosecution. Additionally, ISD immediately took the following corrective actions:

- Notified ARIN to change ownership back to the County of Los Angeles.
- Requested AT&T's assistance in notifying Internet Service Providers (ISP) to discontinue routing traffic through the hijacked addresses.
- Placed controls on the external use of the addresses to allow the County to control and delete any external Internet traffic using these addresses.

It is important to note that the County network was not breached in this incident and all activity took place outside the County environment on the Internet. County data was not threatened or exposed during the time the Internet addresses were hijacked. Similar to Identity Theft, this attack utilized a County of Los Angeles identifier to conduct activities unknown to and not approved by the County. County addresses were not the only Internet addresses inappropriately used in this event; however, it is not known what actions were taken by other victims whose addresses were hijacked. Actions taken by the County will prevent further abuse of these County assets in the future and the Internet registration authority (ARIN) is taking steps to be more diligent in identifying change authority for Internet addresses.

If you have further questions, please contact me at 213.974.2008 or by email at jfullinwider@cio.co.la.ca.us. I will keep you appraised if additional information becomes available.

JWF:ygd

c: Chief Administrative Officer
Interim Director, Internal Services Department
County Counsel
Auditor-Controller
Mark Gascoigne, General Manager, ISD/ITS
Al Brusewitz, Chief Information Security Officer, CIO
Chair, Information Systems Commission